René Mulder

[rene.mulder@forgerock.com](mailto:rene.mulder@forgerock.com)

December 13th 2012

V0.1

# SSO with Citrix XenApp hosted by Windows

## Summary

Achieving Single Sign On for ENIQ Stats BO Win Clients accessed through Citrix is not possible with OpenAM without extensive changes to Business Objects and a migration of the account store.

Achieving Single Sign On for OSS-RC Win Clients accessed through Citrix is based on authentication with Active Directory. There are possibilities to use certificates to authenticate the user, however this requires the userIDs of each identity to be exactly the same in both ComINF LDAP and Active Directory.

Contents

[SSO with Citrix XenApp hosted by Windows 1](#_Toc343166656)

[Summary 1](#_Toc343166657)

[Introduction 3](#_Toc343166658)

[Contents 3](#_Toc343166659)

[Current Situation 3](#_Toc343166660)

[TOR Single Sign On 3](#_Toc343166661)

[Citrix Environment 4](#_Toc343166662)

[Problem statement 5](#_Toc343166663)

[Line of reason of initial approach 5](#_Toc343166664)

[Problem Analysis 6](#_Toc343166665)

[OSS RC Windows Desktop Apps 6](#_Toc343166666)

[ENIQ Stats BO 7](#_Toc343166667)

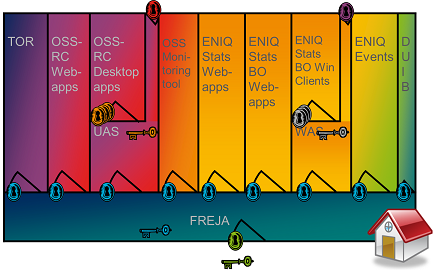
[Appendix: Versions 8](#_Toc343166668)

## Introduction

### Contents

This document contains the problem statement for designing a Single Sign-On solution for applications deployed on Windows Application Server accessed with Citrix in combination with OpenAM.

This is depicted by “**ENIQ Stats BO Win Clients”** in figure 1. There are also some OSS-RC Desktop applications on Windows. These are not in the figure, but are discussed in this document.



1. FREJA House overview

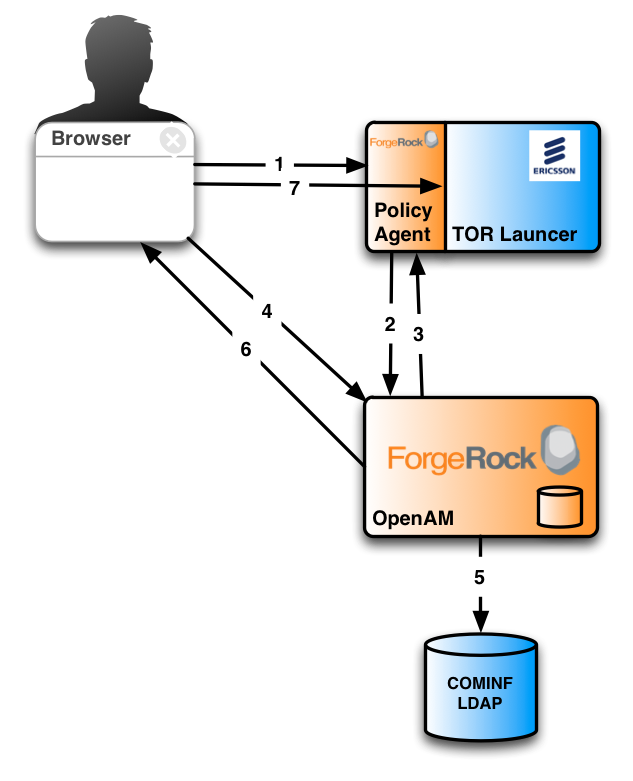
## Current Situation

### TOR Single Sign On

Ericsson has an OpenAM implementation and use OpenAM Policy Agents to secure access to web-applications.

A Policy agent is installed on a webserver or application container. When a user tries to access the web application, the policy agents intercepts the traffic and redirects to OpenAM. OpenAM will handle authenticating the user to the COMINF LDAP.

On subsequent requests, the Agent will recognise the user by its cookie and allow access directly.



1. Standard OpenAM – Agent SSO flow

### Citrix Environment

Citrix provides a proprietary mechanism for SSO, but that is not available since a key component of that Citrix SSO solution is not available. The Citrix web portal is not used. There is no existing SSO based on Citrix technology over the different Citrix applications. In the current environment, static, standard ICA filesare generated on a custom-built server. The ICA files point to the Citrix Farm server to assign the client to one of the Windows based application servers (WAS).

The Citrix receiver directly connects to the Windows machine and starts the application over the ICA protocol.The BO Applications running on the WAS then authenticate the user by presenting a login screen and verifying its validity against an identity store that is not the COMINF LDAP.

Which identity store is used differs per application:

* BO applications use an SQL server on the Business Objects Server
* OSS RC applications WinFIOL and NetAPP use Active Directory

Since the Citrix mechanism is a closed system, there is no way to go beyond configuration of existing features. Even though it is possible to add additional parameters to the ICA file (such as tokens) there is no way to tell the Citrix XenApp software how to use these additional parameters.

## Problem statement

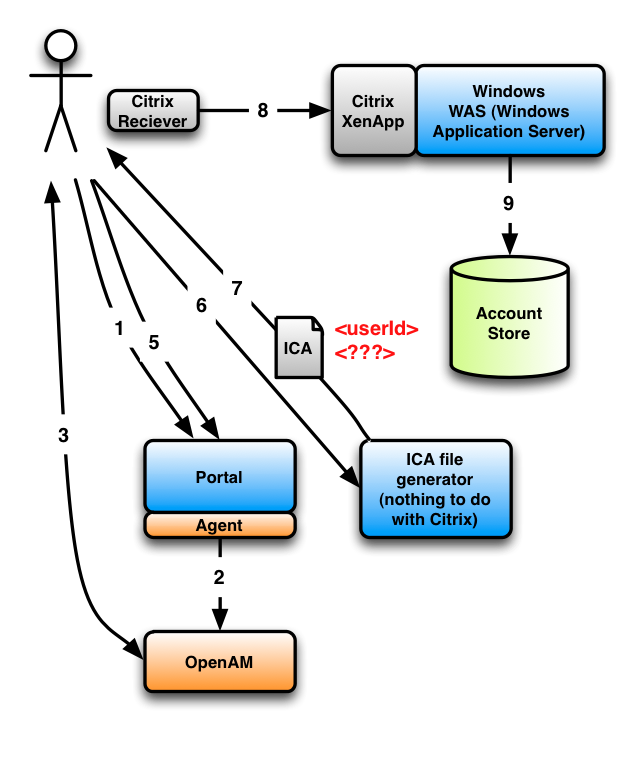
The challenge is to re-use the OpenAM session set up by logging into the portal when accessing / starting up an application on Windows through Citrix.

### Line of reason of initial approach

TheICA file is now static. It can be shared and reused and is therefore insecure. For an SSO scenario we need to introduce a token into the ICA file, that:

1. Has integrityso it can’t be modified without invalidating it
2. Specific to the username that is also in the ICA file
3. Has a time limited validity or can be invalidated externally (by the OpenAM server for example)

This token must be picked up by the XenApp server and verified. Since the XenApp server can’t be modified to use any custom attribute, we will use the ClearPassword attribute.



1. Login flow for Citrix Windows based applications

## Problem Analysis

### OSS RC Windows Desktop Apps

OSS RC Windows Desktop applications authenticate to Active Directory.   
The authentication methods that Active Directory support that do not require a password to be entered are:

1. Kerberos TGT
2. X.509 certificate[[1]](#footnote-1)

Active Directory also supports ADFS[[2]](#footnote-2), but in that scenario AD is the identity provider and not the service provider. Furthermore, Microsoft strategic efforts seem to be moving from ADFS towards the Forefront product stack (FIM and UAG).

Kerberos does not seem to be a logical solution, since OpenAM does not natively support requesting, storing and re-using a TGT when authenticating to Active Directory. Furthermore, the TGT is not secure because it’s not specific to the service that is requested. If intercepted, the attacker can use the TGT to access all services that the user has authorizations.

The certificate based solution could be investigated. However, that goes outside of OpenAM altogether. The certificate should be issued by a CA, which OpenAM is not.

Lastly, for the certificate based solution to work, the user ID in Active Directory needs to be exactly the same as the user ID of the corresponding user in the COMINF LDAP.

### ENIQ Stats BO

ENIQ Stats BO authenticate against an SQL Anywhere server. The data in that server is encrypted. The clients that are able to read and write to the server are BO native applications.

There is no support for the BO application to authenticate in a custom method that would allow verifying a custom token.

Business Objects does support other types of identity stores, such as Active Directory and some other LDAP servers. Moving towards an Active Directory as an identity store results in a similar situation as OSS RC Windows Desktop Apps. Such a migration is a complicated and costly project on the side of Business Objects and even then the solution is not proven. Furthermore, migration to another identity store is planned, but is based on OpenDJ and is planned after the 13B release.

## Appendix: Versions

Ericsson uses:

* Citrix XenApp 5
* Windows 2008 SP2
* Active Directory 2008 SP2
* Citrix Receiver 12

I have both the XenApp 5 reference document available (14MB) as well as the entire WAS Farm server installation manual.

1. <http://social.technet.microsoft.com/Forums/en-US/winserversecurity/thread/0291dee1-1b10-4139-b36d-f1b953f8a09a/> [↑](#footnote-ref-1)
2. <http://en.wikipedia.org/wiki/Active_Directory_Federation_Services> [↑](#footnote-ref-2)